

*NSC REVIEW
COMPLETED*

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

DD/A Registry
File *Security*

DD/A Registry
77-5715/1

15 November 1977

STATINTL

MEMORANDUM FOR: [REDACTED]
Office of General Counsel

STATINTL

FROM: [REDACTED]
Assistant for Information, DDA

SUBJECT: Proposed National Security Council Directive
Concerning National Security Information and
Material

REFERENCE: Multiple addressee memorandum dated 26 October
1977, same subject

STATINTL

1. This paper contains the combined comments of the Office of
Security, Information Systems Analysis Staff, and this office on the
subject draft. We have limited the comments to the undated draft of
[REDACTED] because we feel it is far superior to the [REDACTED] original. STATINTL

Page 2: C. Authority to Classify.

We are pleased to see the provision for classification
authority in the absence of the designee.

Page 2: F. Extension of Classification Beyond Six Years.

We are under the assumption, based on the last meeting on
the Executive Order, that the "demonstrable need" phrase in the
Order was to be changed. If so, it should not be used here.
We suggest the same language be used as in the definition: "at
least significant damage" would result if declassified.

Page 3: G.(1) Identity of Classifier.

Since the Agency uses employee numbers to identify classifi-
cation authorities, request the first sentence read, "be identi-
fied on the face of the information by name, position title or
other identifier."

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

Page 3: G.(2) Date for Declassification or Review.

What happens to documents if they are marked for review by a particular date but are not reviewed for administrative reasons? Throughout the draft there seems to be a presumption against classification. The Agency could not tolerate a system in which documents become declassified automatically if the review date slips by.

Page 4: G.(3) Overall and Page Markings of Documents.

The first sentence at the top of the page indicates that individual pages of a document will be marked with the highest classification of the content of the page. We don't feel that is really necessary if each paragraph of the document is marked individually. Also, this raises the problem of documents printed on both sides. We recommend that every page of a document carry the highest classification of any single paragraph contained therein.

Page 5: G.(5) Waiver of the Portion (Paragraph) Marking Requirement.

We understand the rationale for placing the waiver authority at the SI00 level, but we think the ultimate authority for an agency's documents belongs more appropriately with the head of the agency. In addition, the list of information elements required to seek a waiver needs to be simplified. Item (e) seems absurd, at least in the area of intelligence. Priorities change and what may have seemed a final product suddenly becomes an input to an urgent report. It is difficult, if not impossible, to estimate today what documents may form a basis for derivative classification of other documents tomorrow.

Page 5: G.(6) Subjects and Titles.

We feel the last sentence of this section is unnecessary since we've already said that subjects and titles will be marked with their classifications.

Page 6: G.(7) Material Other Than Documents.

We think the following addition to the end of the sentence would clarify the meaning: "furnished to recipients and stored with the material."

Page 6: G.(10) Declassification, Downgrading, and Upgrading Markings.

The beginning of the last sentence on the page should be changed to conform to J.(1) on page 18 and several other places in the directive. "Known holders or recipients...." We feel this is a very significant point.

Page 8: H. Additional Markings Required.

We notice the deletion from this list of the marking "National Security Information." We think it should be included. EO 11652 prescribes this marking for information or material furnished to persons outside the Executive Branch. The Agency uses it on information furnished to contractors and similar kinds of information.

Page 9: B. Marking.

The derivative classification marking causes us a problem. We can foresee a bibliography of classification sources for each intelligence analyst's reports longer than the report itself. Therefore, the sentence in the middle of the paragraph which reads "In these cases, the record copy of the derivatively classified information shall identify each source of classification applied to the newly prepared information." should end with the words "where practicable" to reduce the burden on our analysts.

Page 10: C. Accountability.

The statement as it now reads implies that the derivative classifier is responsible for the original classification decision. We suggest the following be appended to the sentence: "to the extent they can verify the accuracy of the original classification."

Page 12: A. Emphasis on Declassification.

There is no indication as to who authorizes declassification authority. Also, this section directs that rosters of declassification officers be subject to SIOO review. To protect those officers in a cover status, the same language should be used here as in section D. on page 2: "In cases where listing of the names of officials having classification authority might disclose intelligence information, the Agency shall establish some other record by which such officials can readily be identified."

Page 12: Earliest Possible Declassification.

The words "or event" seem to have been dropped from the first sentence, after "at the earliest possible date."

Page 13: C. New Material.

As we mentioned in our comments on page 3, G.(2), the presumption against classification is apparent in this section. It appears that if through oversight an item of information is left out of the declassification guidelines, it is declassified automatically. We suggest the following addition to the last sentence: "or officially added to the guidelines, if appropriate."

Page 13: D. Old Material.

The same addition above should be added to the sentence, "Information not identified in the guidelines as requiring review shall be declassified." The last word of the last sentence should be changed to "material" to be consistent.

Page 13: E. Declassification Guidelines.

The second sentence is unclear. What is meant by "exclusive in nature"? We feel the sentence is better as follows: "The guidelines shall list the categories of information which require review...."

Page 14: E. Declassification Guidelines (continued)

The first sentence of the page assumes that the Archivist holds and reviews all retired records. This is not so -- we handle our own. We do not want other agencies applying our guidelines to CIA documents found in their records holdings. In any event, the last sentence seems to violate the third agency rule.

Page 14: F. Systematic Review.

This section should be consistent with the proposed Executive order. Section 4.D. of the draft states that only the "permanently valuable" holdings must be reviewed. This phrase should be added to the first sentence in the section. The third sentence contains the "demonstrable damage" phrase (see comment for page 2, F.). Depending on the exact working of the order, this phrase will need to be changed.

Page 15: F. Systematic Review (continued)

The comments above on "demonstrable need" apply here.

Page 15: G.(1) Action on Initial Request.

In order to avoid confusion, the third sentence should read, "The receiving office or office which has been assigned action" In CIA, one office receives and acknowledges the requests and assigns action to other components.

Page 16: G.(3) Availability of Declassified Information.

The Privacy Act should also be cited here.

Page 17: I. Challenges to Classification.

The first sentence reads poorly. We suggest the following partial change, "...information is unnecessarily classified or for which overly restrictive periods...."

Page 18: J.(2) Upgrading of Classification.

This paragraph seems to ignore the problem of those persons who have had access to the material in the past. We suggest the following sentence be added to the end of the paragraph: "Personnel no longer authorized access should be advised, with appropriate admonitions, about the sensitivity of the information in question."

Page 21: C.(2) Dissemination of Intelligence Information.

We recognize that the wording of this section comes verbatim from the current NSCD but the new directive could be improved to ensure compliance. We suggest the addition of the phrase "or his designee" following "an assessment by the senior intelligence official" to ease the administrative burden on the DCI.

Page 22: E. Limitations and Prohibitions on Reproduction.

We understood from [] that paragraph (5) on the recordkeeping for reproduction of Secret and Top Secret documents would be deleted. In addition, in paragraph (6) the words "thermofax or similar" should be deleted. We believe "thermofax" is a registered trademark and cannot be used. Also, there is similar equipment which does not retain an image. There are protective measures which can be taken to avoid security hazards (e.g., vault storage, a daily cleaning of the drum after use, etc.).

Page 23: F.(3) Standards for Security Equipment.

The Office of Security prefers that no exceptions be granted for security equipment. However, if exceptions are to be granted it should be specified that the storage equipment is to be in "CSA approved" steel filing cabinets, whether with combination lock or steel lock bar.

Page 24: F.(5)b. Equipment Out of Service.

It seems that this paragraph providing instructions on how to reset lock combinations on equipment taken out of service is not germane to this document and should be deleted.

Page 26: G.(2) Transmission of Top Secret.

As presently stated, the entire government community is constrained to act according to the Executive Order while the FBI would be free to act as they see fit in the absence of expressed reservations from originating agencies. We do not believe that exceptional authority should be granted to the Director, FBI and suggest that the last five lines of this paragraph be deleted.

Page 27: G.(3)b. Other Areas, Vessels, Military Postal Service, Aircraft.

It should be stipulated that Secret information may be transmitted by United States citizen captains or masters of vessels of United States registry.

Page 27: G.(4) Transmittal of Confidential.

We take exception to the approval of first class mail for transmittal of Confidential material within the United States. Only certified mail should be used for transmission of classified information.

Page 28: G.(6) Telecommunications Conversations.

The reference on the last line should read "subsection G.(2) above."

STATINTL

2. Any questions regarding these comments may be referred to [redacted] We assume a revised directive incorporating the appropriate comments will be circulated for review prior to issuance.

STATINTL

STATINTL

AI/DDA [redacted] dc (15 Nov 77)

Distribution:

Original - Addressee

1 - ISAS/RAB [redacted]

1 - ISAS/RRB

1 - OS/PPG

✓ 1 - DDA Subject w/background (DDA 77-5715)

1 - HGB Chrono

1 - EML Chrono

STATINTL

CONFIDENTIAL

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

3 November 1977

STATINTL

MEMORANDUM FOR: [REDACTED]
Office of General Counsel

STATINTL

FROM : [REDACTED]
Acting Chief, Records Review Branch

SUBJECT : Comments on Proposed National Security
Council Directive

1. Page 1, Para A: Classification Requirements:

Would like to see the second classification criteria eliminated ("the classifier must determine that public disclosure of the particular information meeting a criterion could reasonably be expected to cause at least a significant degree of damage to the national security"). Do not believe that this is a workable criteria.

2. Page 12, Para A: Emphasis on Declassification:

The draft states that declassification authority must be granted in writing. Question? Who grants this authority?

3. Page 13, Para D: Old Material:

This paragraph states that, "Information not identified in the guidelines as requiring review shall be declassified." Since it is impossible to cover everything in a guideline (at least initially) suggest that a provision for guideline modification be included.

4. Page 13, Para E: Declassification Guidelines:

I am not sure that I understand the second sentence. If it means that we will list information by category and not review all categories, then I am for this but would like a clarification.

5. Page 14, Para E: Declassification Guidelines:

a. Doesn't the second sentence conflict with the Executive Order?

CONFIDENTIAL

CONFIDENTIAL

b. Third sentence, the criteria for classification extension, "that declassification of the information would result in demonstrable damage to the national security." This should be changed since it is unable.

c. The sixth sentence: Believe that instead of stating that the Director of Central Intelligence May request request a waiver to the 10-year rereview requirement, that we should push for the wording, the Director of Central Intelligence may authorize a waiver to the 10-year rereview requirement.

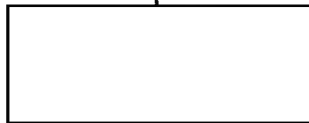
6. Page 17, Para H: Foreign Originated Information:

Do we really want the Department of State in on this?

7. Page 18, Para J(2): Upgrading Classification:

This may not always be possible.

STATINTL



DISTRIBUTION:

Orig. - Adse

✓

[Redacted] O/AI/DDA

1 - RRB Subject

1 - RRB Chrono

STATINTL

CONFIDENTIAL

STATINTL

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

DD/A Registry

20015-1 S 7/5

26 October 1977

STATINTL

MEMORANDUM FOR:



of Security, DDA
Information Services Staff, DDO
and Coordination Staff, DDO
Assistant for Information, DDA
Information Systems Analysis Staff, DDA
Director of Central Reference, DDI
Assistant, DDS&T

STATINTL

FROM



Office of General Counsel

SUBJECT : Proposed National Security Council Directive Concerning
National Security Information and Material

STATINTL

1. Attached are two proposals for implementing the Executive Order that is to replace Executive Order No. 11652. The accompanying note to me from [redacted] participant on the group that drafted these directives, requests any comments to be submitted to him by early November before the directive is forwarded to the NSC.

2. Some general comments about what should be included in such a directive have already been submitted to me, and I am not requesting additional remarks, especially regarding an implementing directive for an Order that has not yet been finalized. However, if you wish me to transmit your comments to Don for possible inclusion in the draft, I would be glad to do so when I make suggestions of my own.

3. The "politics" of drafting which Don mentions refers to the difficulty involved in making any changes in such directives even when they have been circulated for official comment, as they shall be at a later date. I believe Don is suggesting that we should attempt to make our changes now rather than later. While I don't urge anyone to "burn the midnight oil" in order to respond, please call me [redacted] by Thursday, 3 November 1977, if you have any comments. STATINTL

STATINTL



cc: Acting Deputy Director for Administration
Deputy Director for Intelligence
Deputy Director for Operations
Deputy Director for Science & Technology

NATIONAL SECURITY COUNCIL
DIRECTIVE
CONCERNING
NATIONAL SECURITY INFORMATION AND MATERIAL

The President has directed that Executive Order _____, "National Security Information and Material," be implemented in accordance with the following:

I ORIGINAL CLASSIFICATION

A. Classification Requirements. A determination to classify requires the application of a two-step procedure. First, the classifier must determine that the information is classifiable on the basis that it falls within the ambit of one or more of the criterion listed in Section 2(b) of the Order. The criterion listed in the Order are the only standards upon which the classifiability of information may be based. Second, the classifier must determine that public disclosure of the particular information meeting the ^a criterion could reasonably be expected to cause at least a significant degree of damage to the national security. In no case shall information which does not meet both of these requirements be classified.

B. Prohibitions. Heads of Agencies shall take appropriate measures to ensure that all personnel involved with classified information fully understand that violations of Section 2(c) of the Order form an unequivocal basis for imposition of the administrative sanctions of Section 8 of the Order.

C. Authority to Classify. Classification authority is vested in the official designated, and, in the case of designation by position title, in the incumbent of the designated position. In the absence of the designee, classification authority of the designee may be exercised by the individual specifically designated to act in his or her absence.

Where designation is made by position, heads of Agencies shall ensure that adequate records are maintained sufficient to identify at some future date the official who exercised classification authority while in the position.

D. Record Requirements. Each Agency head granted original classification authority pursuant to Section 2(d) of the Order shall cause to be maintained a current listing by classification designation of officials designated in writing as classification authorities. This listing shall be subject to review by the Security Information Oversight Office at any time. In cases where listing of the names of officials having classification authority might disclose intelligence information, the Agency shall establish some other record by which such officials can readily be identified.

E. Accountability. Each official designated as an original classification authority shall be held accountable for the propriety of the classifications attributed to him/her.

F. Extension of Classification Beyond Six Years. The authority to extend the classification of information beyond six years is limited to officials designated in writing as original Top Secret classifiers and to the heads of Departments specified in Section 2(d) of the Order. Such action shall be taken only upon a determination by such officials that a demonstrable need exists for continued protection beyond six years in the interest of national security. Authorities making such extensions shall determine the earliest possible date following the origination of the information upon

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

which it may be declassified. This date shall be entered upon the document. In no case shall the date applied to an original classification action exceed 20 years. In those cases where the information falls within the ambit of declassification guidelines issued by heads of Agencies setting forth specific classes of information which require review on their 20th anniversary prior to declassification, heads of Agencies and Top Secret classification authorities may, only after a determination that earlier declassification cannot be undertaken, specify a date for review of the information in accordance with the guidelines.

G. Standard Identification and Markings. Information originally classified pursuant to the Order shall, at the time of origination, be marked as follows:

(1) Identity of Classifier. The official authorizing the original classification must be identified on the face of the information by name or position title. The identity of the classifier, unless he is also the identified signer or approver of the information, shall be shown on a "classified by" line, e.g., "Classified by (John Doe)" or "Classified by Director, DDR & E".

(2) Date for Declassification or Review. The date or event for automatic declassification of the information or the date for mandatory review of the information for declassification shall be specified on the face of all information classified on or after the effective date of the Order, e.g., "Declassify on 1 May 1983" or "Review for Declassification on 1 March 1998".

(3) Overall and Page Marking of Documents. The overall classification of a document, whether or not permanently bound, or any copy or reproduction thereof, shall be conspicuously marking, stamped, or

permanently affixed at the top and bottom of the outside of the front

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). Each interior page of a classified document shall be conspicuously marked or stamped at the top and bottom according to the highest classification of the content of the page, including the designation "Unclassified", when appropriate.

(4) Portion (Paragraph) Marking. Classifiers shall, through marking or other means, identify (a) the level of classification of each classified portion of a document, and (b) those portions which are not classified. Portion or paragraph marking shall be parenthetical and shall be placed so as to immediately precede the text of each respective portion. The symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be used for this purpose. The symbols "(RD)" and "(FRD)" shall be used in conjunction with the foregoing symbols to identify Restricted Data and Formerly Restricted Data respectively, when applicable, e.g., "(SRD)" for Secret-Restricted Data, or "(CFRD)" for Confidential-Formerly Restricted Data. When portion or paragraph marking is impracticable, classifiers may, through the use of a separate paragraph or conspicuous notation in or on the document, specify the classification level of the various information contained within the document. When all parts of a classified document are classified at the same level and the parts have not been separately marked, a statement to that effect shall be included in the document.

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

(5) Waiver of the Portion (Paragraph) Marking Requirement. The requirement to mark portions or paragraphs of all information classified after the effective date of the Order shall be mandatory unless a specific waiver of this requirement is granted by the Director of the Security Information Oversight Office. Requests for such waivers shall be directed by the head of the Agency to the Director of the Security Information Oversight Office along with (a) specific identification of the information for which such waiver is sought, (b) detailed justification explaining why the Agency should not comply with the marking requirement, (c) the cost impact which would be imposed on the Agency by required marking, (d) the anticipated dissemination of the information, and (e) the agency's best judgement as to the extent that the information may form a basis for derivative classification of other documents.

(6) Subjects and Titles. Whenever possible, subjects and titles shall be selected so as not to require classification. Subjects and titles of classified documents shall be identified as to their classification status by use of the parenthetical symbols shown in (4) above except that such symbols shall be placed immediately following the text of the subject or title. When the subject or title is classified, short titles, consisting of the first letter of each word in the subject or title shall be assigned to facilitate receipting and reference purposes. Subjects or titles of documents created after the effective date of the Order for which the classification status of such subjects and titles has not been indicated shall be considered unclassified.

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

(7) Material Other than Documents. If the classification designation of material other than documents cannot be affixed by marking, stamping, tagging or otherwise, written notification of the security classification shall be furnished to recipients.

(8) Transmittal Documents. A transmittal document, including endorsements and comments, shall indicate on its face the highest classification of the information transmitted by it, and a legend showing the classification, if any, of the transmittal document, endorsements or comments standing alone. For example, in the case of an unclassified document which transmits as an enclosure or an attachment a classified document, the unclassified transmittal document should bear a notation substantially as follows:

"REGRADED UNCLASSIFIED WHEN SEPARATED
FROM CLASSIFIED ENCLOSURE"

(9) Wholly Unclassified Material Not Usually Marked. Normally, wholly unclassified information need not be marked or stamped "Unclassified" except where declassification action has been taken on the information or the marking "Unclassified" will serve the purpose of making clear to the recipient that the originator has made a purposeful determination not to classify it.

(10) Declassification, Downgrading, and Upgrading Markings. Whenever a change is made in the original classification or in the dates or events for downgrading and declassification of any classified information, it shall be promptly and conspicuously marked to reflect the change, the date of the action, the authority for the action, and the identity of the official authorizing the action. Holders or recipients

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

of the information shall be notified of the change. In addition, all earlier classification markings shall be cancelled, if practicable, but in any event such change shall be made on the first page.

(11) Limited Use of Posted Notice for Large Quantities of Information.

When the volume of information is such that prompt remarking of each classified item could not be accomplished without unduly interfering with operations, the custodian may attach declassification, downgrading, or upgrading notices to the storage unit in lieu of the remarking action otherwise required. Each notice shall indicate the change, the authority for the action, the date of the action, the identity of the person taking the action, and the storage units to which it applies. When individual items are withdrawn from such storage units they shall be promptly remarked in accordance with (10), above.

(12) Transfer of Stored Quantities Covered by Posted Notice. When information subject to a posted downgrading, upgrading or declassification notice is withdrawn from one storage unit solely for transfer to another, or a storage unit containing such information is transferred from one place to another, the transfer may be made without remarking if the notice is attached to or remains with each shipment.

H. Additional Markings Required. In addition to the foregoing marking requirements, the following markings shall be prominently displayed on classified information as prescribed below. When display of these additional markings on the information is not feasible, their applicability to the information shall be included in the written notification of the assigned classification.

(1) RESTRICTED DATA. For classified information containing Restricted Data as defined in the Atomic Energy Act of 1954, as amended:

"RESTRICTED DATA"

"This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Its dissemination or disclosure to any unauthorized person is prohibited."

(2) FORMERLY RESTRICTED DATA. For classified information containing Formerly Restricted Data, as defined in Section 142 d., Atomic Energy Act of 1954, as amended, but containing no Restricted Data:

"FORMERLY RESTRICTED DATA"

"Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144b., Atomic Energy Act, 1954."

(3) INTELLIGENCE INFORMATION. For classified information revealing classified intelligence sources or methods, the following markings shall be used in addition to and in conjunction with those prescribed in (1) or (2) above, as appropriate:

"WARNING NOTICE-SENSITIVE INTELLIGENCE

SOURCES AND METHODS INVOLVED"

(4) Specific Dissemination and Reproduction Notice. For classified documents which the originator has determined should be subject to specific dissemination and reproduction limitations, the following statement shall be included in the document or on its cover sheet as a special notation separate and apart from the security classification

"Reproduction of this document or portions thereof is prohibited without authorization of the originating office. Its further dissemination shall be restricted to those authorized by the addressee."

II DERIVATIVE APPLICATION OF MARKINGS

- A. Responsibility. Derivative application of classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form, information which is already classified.
- B. Marking. Derivatively classified information shall show on its face a "Classified by" line which will be completed to show the origin of the classification, e.g., a particular classified document, classification guide or authorized original classifier as the case may be. For information derivatively classified on the basis of multiple sources, the "classified by" line will be completed with the phrase "multiple sources", e.g., "Classified by Multiple Sources." In these cases, the record copy of the derivately classified information shall identify each source of classification applied to the newly prepared information. *where practical* Other marking requirements of the Order and Section I of this Directive shall be observed in all respects. Declassification dates applicable to the source information shall be carried forward to the derivately classified information. In the case of information classified on the basis of multiple sources, the most restrictive of the declassification dates applicable to the various source material used shall be applied to the new information.

New material which is classified on the basis of source material which does not show a date for declassification shall be marked with a date for review for declassification which shall be 20 years from the date of origin of the source material.

C. Accountability. Individuals who apply derivative classification markings shall be held accountable for the accuracy and the necessity of the derivatively applied classifications. *to be held accountable for the accuracy and the necessity of the markings*

D. Control of Derivately Classified Documents. Heads of Agencies shall ensure that Agency education and training programs include training designed to limit, wherever possible, the incorporation of previously classified information in new documents, thereby limiting the number of derivately classified documents.

III CLASSIFICATION GUIDANCE

A. Promulgation. In accordance with the provisions of Section 7(b)(6) of the Order, heads of agencies shall take appropriate measures to ensure the preparation and promulgation of written classification guidance to facilitate the proper and uniform classification of specified information which requires security protection in the interest of national security. Such guidance shall be personally approved in writing by officials with Top Secret classification authority or by heads of Agencies specified in Section 2(d) of the Order.

B. Guidance Requirements. Classification guidance promulgated shall:

- (1) Identify the information elements to be protected, using categorization and sub-categorization to the extent necessary to ensure that the information involved can be readily and uniformly identified;

- (2) State which of the classification designations (i.e., Top Secret, Secret, or Confidential) apply to the identified information element;
- (3) State the duration of each such specified classification in terms of a period of time or future event. When such duration is to exceed six years, the specific reason for such extension shall be annotated on the record copy of the guidance in accordance with the provisions of Section 2(f) of the Order. Where information to be classified for more than six years falls within the ambit of declassification guidelines issued by the head of an Agency, pursuant to Section 4(a) of the Order, the guidance shall require review of the information in accordance with those guidelines at the end of the specified classification period.

C. Review and Report Requirements. All classification guidance shall be reviewed for currency and renewed or revised on an annual basis. Master files of all classification guidance issued by or within each agency listed in Section 2 of the Order shall be compiled and maintained at a central point in each agency for use in fulfilling agency responsibilities for oversight and administration pursuant to Section 7(b)(3) or 7(b)(4) of the Order. Agencies shall also prepare and maintain in a current status separate indices for classified and unclassified classification guidance issued by or within agencies. Copies of the unclassified index shall be provided on an annual basis to the Security Information Oversight Office for compilation and dissemination to interested agencies. The classified index shall be subject to review by the Oversight Office during its regularly scheduled oversight visits and inspections.

Handwritten note:
P. 12
classified
info in
index
in 12/1/80

IV DECLASSIFICATION

- A. Emphasis on Declassification. Heads of Agencies shall cause action to be taken within their agencies which will ensure that emphasis is afforded to declassification consistent with the provisions of Section 4 of the Order. Declassification authority shall be granted in writing to officials at the lowest practicable echelons of command and supervision. Rosters shall be maintained of such authorizations and such rosters shall be subject to review by the Security Information Oversight Office. *In cases where P & do protect covering under.*
- B. Earliest Possible Declassification. Official information shall be declassified at the earliest possible date *or event* following its origination consistent with national security needs. The determination of this earliest possible date or event shall be based not on the level of its assigned classification designation, but rather, on the perishability of the information and the loss of sensitivity which may be expected to occur with the passage of time. Original classifiers may specify declassification dates or events at the limit of their authority only where a specific determination has been made that earlier declassification cannot be accomplished.
- C. New Material. New material, the classification of which is derived from source material classified prior to the effective date of the Order, shall carry forward dates or events for declassification shown on the source material provided such dates or events are not in excess of twenty years from the time of original classification. When the source material is marked for declassification in excess of twenty years from date of origin or bears no declassification date or event, the derivatively classified new material shall be marked for review on a date corresponding to

the twentieth anniversary of the source material. In this review, the declassification guidelines issued by heads of Agencies in effect at the time of the review shall be applied. Information not identified in the declassification guidelines as requiring review on its twentieth anniversary shall be declassified *or officially added to the guidelines, if appropriate.*

9/15/79
D. Old Material. Effective January 1, 1979, information classified under previous Executive orders which is marked for declassification twenty or more years from the time of its origin, or is indeterminately marked shall be reviewed for declassification on its twentieth anniversary. In conducting the review, the declassification guidelines issued by heads of Agencies in effect at the time of the review shall be applied. Information not identified in the guidelines as requiring review shall be declassified. Foreign originated material shall be reviewed on its thirtieth anniversary and declassified in accordance with declassification guidelines covering this *material* ~~information~~.

E. Declassification Guidelines. Heads of Agencies listed in Section 2(d) of the Order shall ensure that declassification guidelines applicable to twenty year old information are prepared and promulgated in accordance with Section 4(a) of the Order. These guidelines shall ~~be exclusive in~~ nature, ~~listing~~ the categories of information which require review on their twentieth anniversary to determine the need for continued protection beyond twenty years, ~~and where applicable, those categories for which the~~ head of an Agency has authorized personally or through his designated representative, extension of classification beyond 20 years, to include declassification or review dates for such extension. ~~Declassification~~ guidelines shall be kept current and reviewed at least annually for that

72

purpose. In order to assure the fullest use of Agency declassification guidelines throughout the Executive branch, each Agency shall furnish a copy of its declassification guidelines and revisions thereto to the Archivist of the United States and to the Security Information Oversight Office. These guidelines shall be made available and authorized for use of other Agencies of the Executive branch as required.

F. Systematic Review. Within a ten year period following the effective date of the Order, Agencies shall have systematically reviewed their holdings of classified information over twenty years old and achieved the goal of conducting systematic review of classified information prior to or upon its twentieth anniversary. Only the head of an Agency or a key official authorized by him in writing shall have the authority to extend classification beyond twenty years. Such extensions shall be made only upon a specific determination that declassification of the information would result in demonstrable damage to the national security. At the time of the twenty year review, information whose classification is authorized to be extended shall be assigned a future declassification date, or if a specific date cannot be determined, a date for subsequent review for declassification which shall not exceed ten years from the date of the twenty-year review. In the latter case, such information shall be re-reviewed at intervals not to exceed ten years until a firm declassification date is determined. Heads of Agencies listed in Section 2(d) of the Order and the Director of Central Intelligence may request a waiver of the ten-year review requirement from the Director of the Security Information Oversight Office. Such requests shall include personal certification by the requester that listed items of information for which the waiver is sought were formally reviewed on their twentieth anniversary,

that a definitive date for their declassification cannot be determined, and that the results of the review established a demonstrable need to retain classification in the interest of national security for a period in excess of twenty additional years. *confusing*

G. Mandatory Review. As required by Section 4(e) of the Order, heads of Agencies shall ensure that procedures are established to process requests for declassification review received from an Agency or member of the public. Such procedures shall conform to the following:

(1) Action on Initial Request. Each Agency shall designate in its implementing regulations, and publish in the Federal Register, an office(s) to which requests for mandatory review for declassification may be directed. This Office shall, in turn, assign the request to the appropriate office for action. *review office or* The office which has been assigned action shall acknowledge receipt of the request to the requester and shall, within thirty days of receipt of the request, make a determination or shall explain to the requester why further time is necessary. If the request requires the rendering of services for which fair and equitable fees should be charged pursuant to Title 5 of the Independent Offices Appropriations Act, 1952, 65 Stat. 290, 31 U.S.C. 483 a, the requester shall so be notified. Should the Office assigned action determine that under the classification requirements set forth in Section 2(a) of the Order continued classification is required, the requester shall be promptly notified, and whenever possible, provided with a brief statement as to why the requested information cannot be declassified. The requester shall also be notified of his/her right of appeal to an Agency appeal authority including the name, title and address of such authority. If at the end of sixty days from receipt

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

of request for review no determination has been made by the Agency action office, the requester may apply to the Agency appeal authority for a determination.

(2) Action on Appeals. Heads of Agencies, or their designees for the purpose, shall establish procedures to review and act upon all appeals of denials of request for declassification within thirty days of receipt of such appeals. The Agency head or his designated appeal authority shall over-rule previous determinations in whole or in part upon a determination that, continued protection is no longer warranted. If the Agency appeal authority determines that continued classification is required under the provisions of Section 2(a) of the Order, it shall promptly notify the requester.

(3) Availability of Declassified Information. Information or any reasonably segregable portion thereof, which is determined to no longer qualify for classification after consideration under (1) or (2) above, shall be declassified and shall be provided to the requester unless it is determined that the information specifically requires withholding in the public interest in accordance with applicable portions of the Freedom of Information Act, as amended (5 U.S.C. 552b). *what about PA?*

(4) Action on Requests for Presidential Material. Requests for declassification review pertaining to material originated by a President or a President's White House staff, or material in the possession and control of the Administrator of General Services pursuant to Section 2107 or 2107 note of title 44, U.S.C., which material is ten or more years old, shall be referred to the Archivist of the United States for disposition in accordance with Section 4(g)(7)

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

of the Order and the requester so notified. The declassification review of such material shall be accomplished in accordance with procedures established by the Archivist. In the case of a denial the requester shall be notified of his or her right to appeal to the Security Information Oversight Office.

H. Foreign Originated Information. The Department of State shall, as appropriate, assist other Agencies with the development of agreements and/or guidelines with respect to the declassification of foreign originated information in the possession of the United States.

I. Challenges to Classification. Agency programs established in implementation of the Order shall encourage holders of classified information to challenge the originators of such information in cases wherein they have substantial reason to believe that the information is unnecessarily classified ^{for which} ~~or~~ overly restrictive periods for continued classification have been assigned. Challenges may also be forwarded through the Security Information Oversight Office which shall promptly forward such challenges to the appropriate Agency for consideration. Agencies shall establish procedures to act on such challenges within 30 days of receipt and to notify the challenger of the results.

J. Changes in Level or Duration of Classification.

(1) Downgrading of Classification. Original Top Secret or Secret classification authorities may, at the time of original classification, provide for automatic downgrading of Top Secret or Secret information to a lower level if it is determined to be advantageous to do so. Such a determination shall be annotated on the face of the information at the time of classification. Whenever the responsible classification authority determines to downgrade information.

other than as originally specified, prompt notification of such action shall be provided to all known holders of the information.

(2) Upgrading of Classification. The upgrading of classified information to a higher level than previously determined is permitted only when it is determined that (i) all known holders of the information can be promptly notified and that (ii) all known holders of the information are authorized access to the higher level of classification, or, that (iii) the information can be retrieved from all known holders of the information not authorized access to the contemplated higher level of classification. When upgrading of a classification is accomplished by the responsible classifier, prompt notification of such action shall be provided to all known holders of the information.

(3) Change of Duration of Classification. The duration of classification specified at the time of original classification may be extended pursuant to the provisions of Section 2(f) of the Order but only if notification of such action can be received by all known holders of the information prior to the date or event previously set for declassification. A shortening of the duration of classification by the classifier shall be coupled with prompt notification of such action to all known holders of the information.

V SAFEGUARDING

A. General. Official information or material classified under the provisions of the Order shall be afforded a level of protection against unauthorized disclosure commensurate with the level of classification

assigned under the varying conditions which may arise in connection with its use, dissemination, storage, movement or transmission, and destruction.

B. Access Limitations. Only persons whose official Government duties, or contractual obligations to or on behalf of the Government necessitate access to classified information shall be nominated for a personnel security clearance. The number of persons nominated for a personnel security clearance shall be kept to the absolute minimum level consistent with official Government requirements. Except as provided in (3) below, access to classified information shall be granted only in accordance with the following:

(1) Determination of Trustworthiness. The standard which shall be applied to determine whether a person is eligible for access to classified information is that, based on all available information, his reliability and trustworthiness are such that entrusting him with classified information is clearly consistent with the national interest. This determination shall be made based on appropriate investigation as determined by the heads of Agencies in accordance with the standards and criteria of applicable Executive orders.

(2) Determination of Need-to-Know. Subsequent to the determination of trustworthiness, classified information shall not be made available to a person unless the possessor of the classified information establishes in each instance that access is essential to the accomplishment of official Government duties or contractual obligations.

(3) Access by Historical Researchers and Former Officials. In addition to the requirements specified in Section 6(d) of the Order, historical researchers and former officials may be granted access to

classified information or material provided that in each case the head of the originating Agency:

- a. Makes a favorable determination of trustworthiness in accordance with Section B(1) above.
- b. Determines that the information or material requested is reasonably accessible and can be located and compiled with a reasonable amount of effort.
- c. Obtains the individual's written agreement to safeguard the information or material in a manner consistent with the Order and implementing Directives thereunder.
- d. Obtains the individual's written consent to a review of his notes and manuscript for the sole purpose of determining that no classified information or material is contained therein.
- e. Ensures that access is afforded only at Government installations or facilities, repositories of the National Archives and Records Service or other approved classified historical records repositories. For historical researchers, the authorization for access shall be valid for a reasonable period but no longer than two years from the date of issuance unless renewed under regulations of the originating Agency.

C. Dissemination.

(1) Consent of Originating Agency to Dissemination by Recipient.

Except as otherwise provided by Section 102 of the National Security Act of 1947, 61 Stat 495, 50 U.S.C. 403, classified information or material originating in one agency shall not be disseminated outside any other agency to which it has been made available without the

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

consent of the originating agency. The Department of Defense shall be considered as one agency in applying the foregoing rule.

(2) Dissemination of Intelligence Information. Information or material bearing the marking "WARNING NOTICE - SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED" shall not be disseminated in any manner outside authorized channels without the permission of the originating Agency and an assessment by ^athe senior intelligence official ^(or his designee) in the disseminating Agency as to the potential risks to the national security and to the intelligence sources and methods involved.

D. Accountability Procedures. Each Agency shall prescribe such accountability procedures as are necessary to control effectively the dissemination of classified information or material. Particularly stringent controls shall be placed on information and material classified Top Secret.

(1) Top Secret Control Officers. Top Secret Control Officers shall be designated, as required, to receive, maintain current accountability and access records of, and dispatch Top Secret material.

(2) Physical Inventory. A physical inventory of all Top Secret material shall be made at least annually. Heads of Agencies may authorize the annual inventory of Top Secret information in repositories, libraries or activities which store large volumes of such information to be limited to documents to which access has been afforded within the past twelve months and ten percent of the remaining inventory.

(3) Current Accountability. Top Secret and Secret information and material shall be subject to such controls including current accountability records as the head of the Agency may prescribe.

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

E. Limitations and Prohibitions on Reproduction. All classified information and material shall be reproduced sparingly and any general or specific prohibition against reproduction shall be strictly adhered to.

(1) Top Secret information shall not be reproduced without the consent of the originator or higher authority and unless such reproduction is determined to be necessary to the conduct of official business.

(2) Secret information shall not be reproduced without the consent of an official designated to authorize such reproduction as is determined to be necessary to the conduct of official business.

(3) No classified document shall be reproduced if such reproduction is prohibited by the originator and the document has been annotated as in Section B(8)(e) above.

(4) Reproduced copies of classified documents shall be subject to the same accountability and controls as the original.

(5) Records shall be maintained by the reproducing office to show the number and distribution of reproduced copies of Secret and Top Secret documents and those annotated as in Section B(8)(e) above.

(6) Classified documents shall not be reproduced by use of Thermofax or similar equipment which retains an image of the document copied.

*absurd
not exact
wording
per JCS*

*According to
Dr. P. B. ...
... set*

*Trademark
no
C. P. ...*

F. Storage. Classified information or material may be stored only where there are facilities or under conditions adequate to prevent unauthorized persons from gaining access to it.

(1) Storage of Top Secret. Top Secret information and material shall be stored in a safe-type steel file cabinet having a built-in three-position dial type combination lock, vault, or vault-type room, or

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

other storage facility which meets the standards for Top Secret established under the provisions of (3) below. In addition, heads of Agencies shall prescribe such additional, supplementary controls as are deemed appropriate to restrict unauthorized access to areas where such information is stored.

(2) Storage of Secret or Confidential. Secret and Confidential material may be stored in a manner and under the conditions prescribed for Top Secret information or material, or in a container or vault which meets the standards for Secret or Confidential, as the case may be, established pursuant to the provisions of (3) or by (4) below.

(3) Standards for Security Equipment. The General Services Administration shall, in coordination with Agencies originating classified information or material, establish and publish uniform standards, specifications and supply schedules for containers, vaults, alarm systems and associated security devices suitable for the storage and protection of all categories of classified information and material. Any agency may establish for use within such agency more stringent standards. Whenever new security equipment is procured, it shall be in conformance with the foregoing standards and specifications and shall, to the maximum extent practicable, be of the type designated on the Federal Supply Schedule, General Services Administration.

(4) Exception to Standards for Security Equipment. As an exception to (3) above, Secret and Confidential material may also be stored in a steel filing cabinet having a built-in, three-position, dial-type changeable combination lock, or a steel filing cabinet equipped with

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

a steel lock bar, provided it is secured by a padlock approved by GSA for the purpose. The storage of Secret information or material in a steel filing cabinet equipped with a steel lock bar, requires the use of such supplementary controls as the head of the Agency deems necessary to achieve the degree of protection warranted by the sensitivity of the information involved.

(5) Combinations.

a. Equipment in Service. Combinations to dial-type locks shall be changed only by persons having appropriate security clearance, and shall be changed whenever such equipment is placed in use, whenever a person knowing the combination no longer requires access to the combination, whenever a combination has been subjected to possible compromise, at least once every year and whenever the equipment is taken out of service. Knowledge of combinations protecting classified information or material shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest level of classified information or material to be stored in the security equipment concerned.

b. Equipment Out of Service. When taken out of service, security equipment having built-in combination locks shall be reset to the standard combination 50-25-50. Combination padlocks shall be reset to the standard combination 10-20-30.

(6) Keys. Heads of Agencies shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated high security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afforded the classified

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

information or material being protected. Under no circumstances shall keys be removed from the premises or stored except in a secure container.

(7) Responsibilities of Custodians. Persons entrusted with classified material shall be responsible for providing protection and accountability for such material at all times and particularly for locking classified material in approved security equipment whenever it is not in use or under direct supervision of authorized persons. Custodians shall follow procedures which insure that unauthorized persons do not gain access to classified information or material by sight or sound. *✓ touch or smell*

(8) Inspections. Individuals charged with the custody of classified information shall conduct the necessary inspections within their areas to ensure adherence to all procedural safeguards prescribed to protect classified information. In addition, Agency security officers shall ensure that periodic inspections are scheduled to ensure that procedural safeguards prescribed by Agency regulations are taken to protect classified information at all times.

G. Transmission.

(1) Preparation and Receipting. Classified information and material shall be enclosed in opaque inner and outer covers before transmitting. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification or its contents. A receipt shall be attached to or enclosed in the inner cover, except that Confidential

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

material shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, addressee, and the document, but shall contain no classified information. It shall be signed by the recipient and returned to the sender.

(2) Transmission of Top Secret. The transmission of Top Secret information and material shall be effected preferably by oral discussion in person between the officials concerned, in an appropriately secure area. Otherwise the transmission of Top Secret information and material shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system especially created for that purpose, over authorized communications circuits in encrypted form or by other means authorized by the National Security Council; [except that in the case of information transmitted by the Federal Bureau of Investigation, such means of transmission may be used as are approved by the Director, Federal Bureau of Investigation, unless express reservation to the contrary is made in exceptional cases by the originating Agency.]

(3) Transmission of Secret. The transmission of Secret material shall be effected in the following manner:

- a. The Fifty States, District of Columbia, Puerto Rico. Secret information and material may be transmitted within and between the fifty States, District of Columbia and Puerto Rico by one of the means authorized for Top Secret information and material, by the United States Postal Service registered mail and by protective services provided by the United States air or surface commercial carriers under such conditions as may be prescribed by the head of the Agency concerned.

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

b. Other Areas, Vessels, Military Postal Service, Aircraft.

Secret information and material may be transmitted from, to or within areas other than those specified in 1. above, by one of the means established for Top Secret information and material, by captains or masters of vessels of United States registry under contract to an agency of the Executive branch, by United States registered mail through Army, Navy or Air Force Postal Service facilities provided that material does not at any time pass out of United States citizen control and does not pass through a foreign postal system, and by commercial aircraft under charter to the United States and military or other government aircraft.

c. Canadian Government Installations. Secret information and material may be transmitted to and between United States Government and Canadian Government installations in the fifty States, the District of Columbia and Canada by United States and Canada registered mail with registered mail receipt.

(4) Transmittal of Confidential. Confidential information and material shall be transmitted within the forty-eight contiguous states and the District of Columbia, or wholly within Alaska, Hawaii, the Commonwealth of Puerto Rico, or a United States possession, by one of the means established for higher classifications, or by certified or first class mail when prescribed by an agency head. Outside these areas, Confidential information and material shall be transmitted only as is authorized for higher classifications.

(5) Transmission within an Agency. Agency regulations governing the preparation and transmission of classified information within an Agency shall ensure a degree of security equivalent to that prescribed above for transmission outside the Agency.

(6) Telecommunications Conversations. Classified information shall not be communicated over telecommunications circuits or systems other than those specifically authorized for transmission of classified information pursuant to subsection ^{TG2}~~(b)(7)~~ above. *copied for*

STAT

H. Loss or Possible Compromise. Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to an official designated by his Agency or organization. In turn, the originating Agency shall be notified about the loss or possible compromise in order that a damage assessment may be conducted and appropriate measures taken to negate or minimize the adverse effect of such a compromise. An immediate inquiry shall be initiated by the Agency under whose cognizance the loss or compromise occurred for the purpose of taking corrective measures and appropriate administrative, disciplinary, or legal action.

I. Destruction. [Non-record] classified information or material which has served its intended purpose shall be destroyed in accordance with procedures and methods approved by the head of the Agency. The method of destruction selected must preclude recognition or reconstruction of the classified information or material.

VI IMPLEMENTATION AND REVIEW

A. Oversight Office. The Security Information Oversight Office established pursuant to Section 7 of the Order shall monitor actions taken by Agencies to ensure effective implementation and adherence to the policies and provisions of the Order and its implementing directives. To this end, the Office shall be responsible for, as amended below, all functions assigned to the Interagency Classification Review Committee (ICRC) pursuant to Executive Order 11652, March 8, 1972. Personnel employed in connection with the performance of functions assigned to the ICRC and the personnel positions, assets, liabilities, property, records, and unexpended balance of appropriations, authorizations and allocations available to or to be made available in connection with the functions transferred to the Oversight Office shall be transferred for appropriate allocation. Personnel shall be transferred in accordance with applicable laws and regulations. The Office shall be responsible for, among others, the following functions:

- (1) Overseeing Agency actions to ensure compliance with the provisions of the Order and implementing directives.
- (2) Obtaining and reviewing Agency implementing regulations and those of subordinate components as may be necessary to determine the effectiveness of Agency implementation.
- (3) Developing and promulgating such reporting requirements as the Director may find necessary for the Oversight Office to carry out its responsibilities and ensuring the timely submission of such reports by Agencies.

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

(4) Considering and taking action on suggestions and complaints from persons within or outside the Government with respect to the general administration of the Order, and in consultation with the affected Agency or Agencies, assuring that appropriate action is taken on such complaints or suggestions.

(5) Considering and taking action on appeals from denials by Agency appeal authorities for the declassification of ten or more year old material originated by a President, a President's White House staff, or material in the possession and control of the Administrator of General Services pursuant to Section 2107 or 2107 note of title 44, U.S.C.

(6) Conducting visits on a scheduled basis to Agencies holding classified material (regardless of whether or not the Agency has been granted original classification authority) to review the practical application of classification and declassification policy and the safeguarding of national security information by officials and employees of those Agencies, and ensuring that appropriate action is taken by Agencies to correct deficiencies noted during such reviews.

(7) Not later than May 1 of each year reporting to the President on the administration of the Order during the preceding calendar year.

(8) Developing and promulgating with the approval of the National Security Council, and in consultation with affected Agencies, policy and administrative directives required for the effective implementation of the Order.

(9) Serving as a clearinghouse for information with respect to the interpretation of the provisions of the Order and its implementing directives.

Approved For Release 2002/08/21 : CIA-RDP80-00473A000600120015-1

(10) Developing ways and means, in coordination with affected Agencies, of standardizing security practices, procedures and administrative forms throughout the Executive branch.

(11) Conducting security symposia and training seminars and publishing periodic security newsletters.

(12) In consultation with Agencies, developing means to (a) prevent overclassification, (b) ensure prompt declassification in accordance with the provisions of the Order, (c) facilitate access to declassified information, and (d) limiting the unauthorized disclosure of classified information.

B. Interagency Security Information Advisory Committee. Members of the Interagency Security Information Advisory Committee established under Section 7(a)(2) of the Order shall be senior representatives of the Agencies represented thereon.

C. Agencies.

(1) Agency Committees. Members of Agency committees established pursuant to Section 7(b)(4) of the Order shall be appointed from among senior officials of the Agency knowledgeable concerning the security classification system established by the Order and significantly responsible for implementation of the system within the Agency.

(2) Reports. Agencies shall submit to the Security Information Oversight Office such oversight reports as the Director finds necessary for accomplishing the responsibilities of the Oversight Office. The first of such reports shall cover the period from the effective date of the Order through December 31, 1978, and shall be submitted to the

Oversight Office no later than 30 days thereafter. Subsequent reports shall be submitted on a semi-annual basis as above covering the periods January 1 - June 30 and July 1 - December 31.

VII COMBAT OPERATIONS

The provisions of the Order and this Directive with regard to dissemination, transmission, or safeguarding of classified information or material may be so modified in connection with combat or combat-related operations as the Secretary of Defense may by regulations prescribe.

VIII ATOMIC ENERGY MATERIAL

"Restricted Data" and material designated as "Formerly Restricted Data" shall be handled, protected, classified, downgraded and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, the Order, this Directive, and the regulations of the Department of Energy issued pursuant to the Act.

IX PUBLICATION AND EFFECTIVE DATE

This Directive shall be published in the Federal Register and become effective March 1, 1978.

DRAFT

NATIONAL SECURITY COUNCIL

5 OCT 1977

D I R E C T I V E

concerning

NATIONAL SECURITY INFORMATION AND MATERIAL

Section A. General. The President has directed that Executive Order #####, "National Security Information and Material," approved (date), be implemented in accordance with this Directive which is structured in the same manner as the Order and is intended to be used as a companion piece to the Order as it does not unnecessarily reiterate the provisions of the Order.

Section B. Original Classification.

(1) Classification Requirements. Classification is a two step process. First, the classifier must determine that the information is classifiable on the basis that it falls within the ambit of one or more of the criterion listed in Section 2(b) of the Order. Secondly, the classifier must determine that disclosure of such information could reasonably be expected to cause at least a significant degree of damage to the national security. In no case shall information be classified which does not meet both of these requirements.

(2) Prohibitions. The prohibitions against classification listed in Section 2(c) of the Order are absolute. Heads of agencies will take appropriate measures to ensure that all original classification authorities fully understand that violations of Section 2(c)

of the Order form an unequivocal basis for imposition of the administrative sanctions of Section 8(b) of the Order.

(3) Authority to Classify. The authority to originally classify official information is restricted solely to those officials specifically designated by, or in writing pursuant to, Section 2(d)(1) through (5) of the Order. It is vested in the official designated, and, in the case of designation by position title, in the incumbent of the designated position. In the absence of the designee, the classification authority may be exercised by the individual specifically designated to act in his or her absence. The exercise of this authority is personal to these officials and except as provided in Section 2(d)(4) of the Order may not be delegated. Authority to classify is limited to the level of classification which is specifically authorized and to any lower level. Designations of this authority shall be limited to the minimum number absolutely required for efficient administration.

(4) Redelelegation of Classification Authority. Authorization to redelegate classification authority shall be limited to senior officials in each Agency and such authorizations must be exercised with restraint.

(5) Record Requirement. Each Agency enumerated in Section 2(d)(1) through (3) of the Order shall provide for maintaining, by name or position title, separate listings of those officials who

have been designated in writing to have Top Secret, Secret and Confidential classification authority. These listings shall be maintained in a current status.

(6) Limitation of Authority to Provide for Duration of Classification. Without need and specific justification, a classification at any level assigned by whatever authority may not be continued in excess of six years. The authority of heads of agencies and Top Secret classifiers to extend beyond six years a classification made by them or by Confidential or Secret classification authorities under their direction or supervision shall be used with prudence.

(a) Heads of Agencies. Except as provided in Section 4(f) of the Order, the heads of agencies enumerated in Section 2(d) of the Order may, at the time of original classification, set any date or event for automatic declassification which date or event shall be within twenty years of the date of original classification. Only heads of such agencies may authorize extension of classification beyond twenty years.

(b) Top Secret Authorities. Except as provided in Section 4(f) of the Order and unless declassification without prior review is expressly prohibited by guidelines issued by the head of agency pursuant to Section 4(a) of the Order, Top Secret original classification authorities may, at the time of original classification, set any date or event for automatic declassification which date or event shall be

within twenty years of the date of original classification. When guidelines issued by the head of an Agency pursuant to Section 4(a) of the Order expressly prohibit declassification without prior review, only Top Secret classification authorities may, at the time of original classification, set a date for review for declassification which date shall be consistent with the guidelines.

(c) Confidential and Secret Authorities. Confidential and Secret original classification authorities may, at the time of original classification, set any date or event for automatic declassification within six years of the date of original classification but may not set a date for review in lieu of automatic declassification.

(7) Identification and Markings. In addition to the proscriptions against substitution of authorized classification designations in Section 2(g)(1) of the Order and except as specifically authorized herein, no term shall be authorized for or used as an adjunct to or in conjunction with the authorized classification designations Top Secret, Secret or Confidential to qualify such designations. Documents classified pursuant to the Order shall, at the time of origination or preparation, be marked as follows:

(a) Identity of Original Classifier. The classifying official must be identified on the face of documents he or she originally classifies. If the signer or approver of such documents is other

than the classifier, the identity of the original classifier shall be shown on a "Classified by" line. In all other instances, the person who signs or finally approves such a classified document shall be deemed to be the classifier. See Section C for identification of classification authority on documents derivatively classified.

(b) Date for Declassification or Review. The date or event for automatic declassification or the date for review for declassification shall be specified on the face of all documents classified on or after the effective date of the Order, e.g., "DECLASSIFY ON 1 May 1983" or "REVIEW FOR DECLASSIFICATION ON 13 November 1997."

(c) Overall and Page Marking of Documents. The overall classification designation of a document, whether or not permanently bound, or any copy or reproduction thereof, shall be conspicuously marked or stamped at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page and on the outside of the back cover (if any). Each interior page of a classified document shall be conspicuously marked or stamped at the top and bottom according to the highest classification designation of the content of the page, including the designation "Unclassified" when appropriate.

(d) Portion (Paragraph) Marking. Each portion or part of a classified document shall, except as otherwise provided in this subsection, be marked to identify its classification or that it is unclassified. The marking shall be parenthetical and shall immediately precede the text of the portion. The symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be used for this purpose. The symbols "RD" and "FRD" shall be used in conjunction with the foregoing symbols for Restricted Data and Formerly Restricted Data, respectively, when applicable, e.g., "(SRD)" or "(CFRD)." If in an exceptional situation, such marking is determined to be impracticable, the document shall contain a description sufficient to identify the exact information which is classified and the levels of classification assigned thereto. When all parts of a classified document are classified at the same level and the parts of the document have not been separately marked, a statement to that effect shall be included in the document.

(e) Subjects and Titles. Subjects and titles shall be selected, if possible, so as not to require classification. Subjects and titles of classified documents shall be identified as to their classification status by use of the appropriate parenthetical symbols shown in (d) above except that such symbols shall be placed immediately following the text of the subject or title.

(f) Transmittal Documents. A transmittal document shall show

on its face both a prominent notation as to the highest classification of the information which is carried with it, and the classification, if any, of the transmittal document standing alone.

(g) Wholly Unclassified Material. Wholly unclassified material shall not be marked or stamped "Unclassified" unless the purpose of the marking is notification of a decision not to classify the material.

(h) Other Material. Classified material in other than documentary form shall bear the foregoing markings, as well as applicable additional markings in subsection (8) below, or the information provided by such markings shall be furnished by accompanying or referenced documentation.

(i) Declassification, Downgrading and Upgrading Markings. Whenever an unscheduled change is made in the originally assigned level of classification or dates or events for downgrading or declassification of any classified document or material it shall be promptly and conspicuously marked to indicate the change, the authority for the action, the date of the action, and the identity of the person taking the action. In the case of downgrading or declassification, earlier classification markings shall be superseded or obliterated on the first page, and, if practicable, throughout a document. In the case of upgrading, the old classification markings shall be superseded on each page.

(j) Limited Use of Posted Notice for Large Quantities of Stored Material. When the volume of information or material is such that prompt remarking of each classified item could not be accomplished

without unduly interfering with operations, the custodian may attach declassification, downgrading or upgrading notices to the storage unit in lieu of the remarking otherwise required. Each notice shall indicate the change, the authority for the action, the date of the action, the identity of the person taking the action and the storage units to which it applies. When individual items are withdrawn from such storage units they shall be promptly remarked in accordance with (i) above.

(k) Transfer of Stored Quantities Covered by Posted Notice.

When information or material subject to a posted downgrading, upgrading or declassification notice is withdrawn from one storage unit solely for transfer to another, or a storage unit containing such material is transferred from one place to another, the transfer may be made without remarking if the notice is attached to or remains with each shipment.

(8) Additional Markings. In addition to the foregoing, the following markings shall be prominently displayed on classified documents or materials as prescribed below. When display of these additional markings on the documents or other materials is not feasible, they shall be included in the written notification of the assigned classification.

(a) Restricted Data. For classified information or material

containing Restricted Data as defined in the Atomic Energy Act of 1954, as amended:

"RESTRICTED DATA"

This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Its dissemination or disclosure to any unauthorized person is prohibited.

(b) Formerly Restricted Data. For classified information or material containing Formerly Restricted Data, as defined in Section 142.d., Atomic Energy Act of 1954, as amended, but no Restricted Data:

"FORMERLY RESTRICTED DATA"

Unauthorized disclosure subject to Administrative and Criminal Sanctions. Handle as Restricted Data in Foreign Dissemination. Section 144.b., Atomic Energy Act, 1954.

(c) Information Other Than Restricted Data or Formerly Restricted Data. For classified information or material furnished to persons outside the Executive Branch of Government other than as described in (a) and (b) above:

"NATIONAL SECURITY INFORMATION"

Unauthorized Disclosure Subject to Criminal Sanctions

(d) Intelligence Information. For information or material revealing classified intelligence sources and methods, the following marking shall be used, in addition to and in conjunction with those prescribed in (a), (b) or (c) above, as appropriate:

"WARNING NOTICE - SENSITIVE
INTELLIGENCE SOURCES AND
METHODS INVOLVED"

(e) Specific Dissemination and Reproduction Notice. For classified documents which the originator has determined should be subject to specific dissemination and reproduction limitations, the following statement shall be included in the document or on its cover sheet as a special notation separate and apart from the security classification marking:

"Reproduction of this document or portions thereof is prohibited without authorization of the originating office. Its further dissemination shall be restricted to those authorized by the addressee."

Section C. Derivative Application of Markings. The derivative application of classification markings is a responsibility of those who incorporate, paraphrase restate or generate in new form, information which is already classified. Derivatively classified information shall show on its face a "Classified by" line which will be completed to show the origin of classification, e.g., a particular previously classified document, a classification guide or authorized classifier as the case may be. For information classified on the basis of multiple sources, the "Classified by" line will be completed with the phrase "multiple sources," i.e.,

"CLASSIFIED BY multiple sources." In this latter instance, the record copy of the derivatively classified material shall identify each source of classification applied to the newly prepared information. Dates or events for declassification or dates for review for declassification shall be brought forward to the newly prepared information in accordance with the provisions of Section 3 of the Order. Other marking requirements and proscriptions of the Order and Sections B(7) and (8) of this Directive shall be observed in all respects.

Section D. Declassification. At the time of original classification, original classifiers shall specify dates or events for declassification which are as early as the national security will permit. Classifiers shall determine such dates after consideration of the perishability of the information and the loss of sensitivity which may be expected to occur with the passage of time.

(1) Declassification Guidelines. Declassification guidelines issued under Section 4 (a) of the Order will be applicable to twenty year old information classified under previous Executive orders and to information classified under the present order as such information becomes twenty years old. These declassification guidelines shall be kept current and shall be reviewed at least annually for that purpose. Each agency shall furnish a copy of its declassification guidelines to the Archivist of the United States and to the Security Information Oversight Office. Agency declassification

guidelines also shall be made available to and authorized for use by other agencies of the Executive Branch as required.

(2) New Material. New material, the classification of which is derived from source material classified prior to the effective date of the Order shall specify dates or events for automatic declassification or review for declassification as determined pursuant to Sections 3 and 4 of the Order and shall be declassified or reviewed for declassification in accordance with such dates.

(3) Old Material. Except as provided in Section 4 (c) of the Order, material classified under previous Executive orders which is marked for declassification in excess of twenty years from the time of its origin, marked with an indeterminate declassification date or not marked with a declassification date, shall be reviewed for declassification twenty years from the time of original classification against the guidelines issued in accordance with Section 4 (a) of the Order.

(4) Systematic Review. Except for that which is foreign originated, systematic review of permanently valuable classified record material more than twenty years old, must be completed within ten years after the effective date of the Order. Thereafter, classified material which becomes twenty years old shall be reviewed on a current basis. If upon review of twenty-year old permanently valuable classified record material it is determined

that the classification of certain of such material is to be continued beyond twenty years, a date for automatic declassification or a date not in excess of ten years later for review of the classification of the information shall be set in accordance with Section 4(d) of the Order pursuant to the authorization of the head of an agency listed in Section 2(d) of the Order.

(5) Mandatory Review. A request for declassification review pursuant to Section 4(e) of the Order must describe the document or material with sufficient particularity to enable the agency to identify and locate it with a reasonable amount of effort. Whenever a request is deficient in its description of the material sought, or the request is of such scope as to be unduly burdensome, the requester should be asked to provide additional identifying information or to narrow the scope of his or her request. If none-the-less the requester does not describe the records sought with sufficient particularity, or narrow the scope of the request, he or she shall be notified of the reasons why no action will be taken. The procedural instructions for processing requests for declassification review are as follows:

(a) Action on Initial Request. Each Agency shall designate in its implementing regulations, and publish in the Federal Register, one or more offices to which members of the public or agencies may direct

requests for mandatory review for declassification in accordance with Section 4(e) of the Order. Within thirty days of receipt of a request for mandatory review for declassification, a requester shall be notified of the determination or the reasons why further time is necessary in order to make a determination. Upon determination that the information or material or any reasonably segregable portion thereof no longer qualifies for classification pursuant to Section 2(a) of the Order, such information or material shall be declassified and provided to the requester unless it is determined that the information or material may be withheld in accordance with applicable provisions of the Freedom of Information Act, as amended (5 U.S.C. 552b) and that it is important to the public interest to do so. A requester shall be promptly notified of a determination that information or material or portions thereof requires continued classification protection pursuant to Section 2(a) of the Order and shall be provided a brief statement as to why the requested information or material cannot be declassified and of his or her right of appeal.

(b) Action on Appeals. Each agency shall establish procedures to review and act upon, within thirty days after receipt, appeals of denials of requests for declassification made under the Order. Appellate determinations shall be handled in the manner prescribed in (a) above.

(c) Fees. Actions taken under (a) or (b) above may require the rendering of services for which fair and equitable fees should be charged pursuant to Title 5 of the Independent Offices Appropriations Act, 1952, 65 Stat 290, 31 U.S.C. 483a. When such fees are appropriate, an advance determination will be made as to whether the requester will pay the cost associated with searching for and duplicating the information or material sought.

(d) Action on Requests for Presidential Papers. A request for declassification review of material which is subject to Section 4(e)(4) of the Order and is less than ten years old, received by an agency, shall be returned to the requester without action together with an explanation that the provisions of Section 4(e)(4) of the Order exempt that class of records from review. A request for declassification review of such records which are ten or more years old, received by an agency, shall be referred to the Archivist of the United States for disposition in accordance with Section 4(g)(7) of the Order and the requester so notified. The declassification review of such material shall be accomplished in accordance with procedures established by the Archivist who shall notify a requester of his or her right to appeal to the Security Information Oversight Office a denial of such a request.

(6) Foreign Originated Information. Agencies which hold in their custody foreign originated classified information or material described in Section 4(f) of the Order shall, in coordination with

the Department of State and Archivist of the United States, develop agreements or guidelines for declassifying such material upon review 30 years after its date of origin. Such agreements or guidelines shall be referred, through the Department of State, to the foreign government involved for review and approval. The declassification review prescribed in Section 4(f) of the Order shall be accomplished in accordance with such mutually accepted agreements or guidelines.

Section E. Changes in Level or Duration of Classification.

(1) Downgrading of Classification. Original Top Secret or Secret classification authorities may, at the time of original classification, provide for automatic downgrading of Top Secret or Secret information to a lower level if it is determined to be advantageous to do so. Such a determination shall be annotated on the face of the information at the time of classification. Whenever the responsible classification authority determines to downgrade previously classified information other than as originally specified, prompt notification of such action shall be provided to all known holders of the information.

(2) Upgrading of Classification. The upgrading of classified information to a higher level than previously determined is permitted only when it is determined that (i) all known holders of the information can be promptly notified and that (ii) all known holders of the information are authorized access to the higher level of classifi-

cation, or, that (iii) the information can be retrieved from all known holders of the information not authorized access to the contemplated higher level of classification. When upgrading of a classification is accomplished by the responsible classifier, prompt notification of such action shall be provided to all known holders of the information.

(3) Change of Duration of Classification. The duration of classification specified at the time of original classification may be extended pursuant to the provisions of Section 2(f) of the Order but only if notification of such action can be received by all known holders of the information prior to the date or event previously set for declassification. A shortening of the duration of classification by the classifier shall be coupled with prompt notification of such action to all known holders of the information.

Section F. Safeguarding. Official information or material classified under the provisions of the Order shall be afforded a level of protection against unauthorized disclosure commensurate with the level of classification assigned under the varying conditions which may arise in connection with its use, dissemination, storage, movement or transmission, and destruction.

(1) Access Limitations. Only persons whose official Government duties or contractual obligations to or on behalf of the Government necessitate access to classified information shall be nominated for a personnel security clearance. The number of persons nominated for a

personnel security clearance shall be kept to the absolute minimum level consistent with official Government requirements. Except as provided in (c) below, access to classified information shall be granted only in accordance with the following:

(a) Determination of Trustworthiness. The standard which shall be applied to determine whether a person is eligible for access to classified information is that, based on all available information, his reliability and trustworthiness are such that entrusting him with classified information is clearly consistent with the national interest. This determination shall be made based on appropriate investigation as determined by the heads of Agencies in accordance with the standards and criteria of applicable Executive Orders.

(b) Determination of Need-to-Know. Subsequent to the determination of trustworthiness, classified information shall not be made available to a person unless the possessor of the classified information establishes in each instance that access is essential to the accomplishment of official Government duties or contractual obligations.

(c) Access by Historical Researchers and Former Officials. In addition to the requirements specified in Section 6(d) of the Order, historical researchers and former officials may be granted access to classified information or material provided that in each case the head of the originating Agency:

1. Makes a favorable determination of trustworthiness in accordance with Section F(1)(b) above.

2. Determines that the information or material requested is reasonably accessible and can be located and compiled with a reasonable amount of effort.

3. Obtains the individual's written agreement to safeguard the information or material in a manner consistent with the Order and implementing Directives thereunder.

4. Obtains the individual's written consent to a review of his notes and manuscript for the sole purpose of determining that no classified information or material is contained therein.

5. Ensures that access is afforded only at Government installations or facilities, repositories of the National Archives and Records Service or other approved classified historical records repositories. For historical researchers, the authorization for access shall be valid for a reasonable period but no longer than two years from the date of issuance unless renewed under regulations of the originating Agency.

(2) Dissemination.

- (a) Consent of Originating Agency to Dissemination by Recipient. Except as otherwise provided by Section 102 of the National Security Act of 1947, 61 Stat 495, 50 U.S.C. 403, classified information or material originating in one agency shall not be

disseminated outside any other agency to which it has been made available without the consent of the originating agency. The Department of Defense shall be considered as one agency in applying the foregoing rule.

(b) Dissemination of Intelligence Information. Information or material bearing the marking "WARNING NOTICE - SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED" shall not be disseminated in any manner outside authorized channels without the permission of the originating Agency and an assessment by the senior intelligence official in the disseminating Agency as to the potential risks to the national security and to the intelligence sources and methods involved.

(3) Accountability Procedures. Each Agency shall prescribe such accountability procedures as are necessary to control effectively the dissemination of classified information or material. Particularly stringent controls shall be placed on information and material classified Top Secret.

(a) Top Secret Control Officers. Top Secret Control Officers shall be designated, as required, to receive, maintain current accountability records of, and dispatch Top Secret material.

(b) Physical Inventory. A physical inventory of all Top Secret material shall be made at least annually. Heads of Agencies may authorize the annual inventory of Top Secret information in repositories, libraries or activities which store large volumes of such

information to be limited to documents to which access has been afforded within the past twelve months and ten percent of the remaining inventory.

(c) Current Accountability. Top Secret and Secret information and material shall be subject to such controls including current accountability records as the head of the Agency may prescribe.

(4) Limitations and Prohibitions on Reproduction. All classified information and material shall be reproduced sparingly and any general or specific prohibition against reproduction shall be strictly adhered to.

(a) Top Secret information shall not be reproduced without the consent of the originator or higher authority and unless such reproduction is determined to be necessary to the conduct of official business.

(b) Secret information shall not be reproduced without the consent of an official designated to authorize such reproduction as is determined to be necessary to the conduct of official business.

(c) No classified document shall be reproduced if such reproduction is prohibited by the originator and the document has been annotated as in Section B(8)(e) above.

(d) Reproduced copies of classified documents shall be subject to the same accountability and controls as the original.

(e) Records shall be maintained by the reproducing office to show the number and distribution of reproduced copies of Secret and Top Secret documents and those annotated as in Section B(8)(e) above.

(5) Storage. Classified information or material may be stored only where there are facilities or under conditions adequate to prevent unauthorized persons from gaining access to it.

(a) Storage of Top Secret. Top Secret information and material shall be stored in a safe or safe-type steel file cabinet having a built-in three-position dial type combination lock, vault, or vault-type room, or other storage facility which meets the standards for Top Secret established under the provisions of (c) below. In addition, heads of agencies shall prescribe such additional, supplementary controls as are deemed appropriate to restrict unauthorized access to areas where such information is stored.

(b) Storage of Secret or Confidential. Secret and Confidential material may be stored in a manner and under the conditions prescribed for Top Secret information or material, or in a container or vault which meets the standards for Secret or Confidential, as the case may be, established pursuant to the provisions of (c) or by (d) below.

(c) Standards for Security Equipment. The General Services Administration shall, in coordination with Agencies originating classified information or material, establish and publish uniform standards, specifications and supply schedules for containers, vaults, alarm systems and associated security devices suitable for the storage and protection of all categories of classified information and material. Any agency may establish for use within such agency more stringent standards. Whenever new security equipment is procured, it shall be

in conformance with the foregoing standards and specifications and shall, to the maximum extent practicable, be of the type designated on the Federal Supply Schedule, General Services Administration.

(d) Exception to Standards for Security Equipment. As an exception to (c) above, Secret and Confidential material may also be stored in a steel filing cabinet having a built-in, three-position, dial-type changeable combination lock, or a steel filing cabinet equipped with a steel lock bar, provided it is secured by a padlock approved by GSA for the purpose. The storage of Secret information or material in a steel filing cabinet equipped with a steel lock bar, requires the use of such supplementary controls as the head of the Agency deems necessary to achieve the degree of protection warranted by the sensitivity of the information involved.

(e) Combinations.

1. Equipment in Service. Combinations to dial-type locks shall be changed only by persons having appropriate security clearance, and shall be changed whenever such equipment is placed in use, whenever a person knowing the combination no longer requires access to the combination, whenever a combination has been subjected to possible compromise, at least once every year and whenever the equipment is taken out of service. Knowledge of combinations protecting classified information or material shall be limited to the minimum number of persons necessary for operating purposes. Records

of combinations shall be classified no lower than the highest level of classified information or material to be stored in the security equipment concerned.

2. Equipment Out of Service. When taken out of service, security equipment having built-in combination locks shall be reset to the standard combination 50-25-50. Combination padlocks shall be reset to the standard combination 10-20-30.

(f) Keys. Heads of Agencies shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated high security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afforded the classified information or material being protected. Under no circumstances shall keys be removed from the premises or stored except in a secure container.

(g) Responsibilities of Custodians. Persons entrusted with classified material shall be responsible for providing protection and accountability for such material at all times and particularly for locking classified material in approved security equipment whenever it is not in use or under direct supervision of authorized persons. Custodians shall follow procedures which insure that unauthorized persons do not gain access to classified information or material by sight or sound.

(6) Transmission.

(a) Preparation and Receipting. Classified information and material shall be enclosed in opaque inner and outer covers before transmitting. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification or its contents. A receipt shall be attached to or enclosed in the inner cover, except that Confidential material shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, addressee, and the document, but shall contain no classified information. It shall be signed by the recipient and returned to the sender.

(b) Transmission of Top Secret. The transmission of Top Secret information and material shall be effected preferably by oral discussion in person between the officials concerned, in an appropriately secure area. Otherwise the transmission of Top Secret information and material shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system especially created for that purpose, over authorized communications circuits in encrypted form or by other means authorized by the National Security Council; except that in the case of information transmitted by the Federal Bureau of Investigation, such means of transmission may be used as are approved by the Director, Federal Bureau of Investigation, unless express reservation to the contrary is made in exceptional cases by the originating Agency.

(c) Transmission of Secret. The transmission of Secret material shall be effected in the following manner:

1. The Fifty States, District of Columbia, Puerto Rico. Secret information and material may be transmitted within and between the fifty States, District of Columbia and Puerto Rico by one of the means authorized for Top Secret information and material, by the United States Postal Service registered mail and by protective services provided by the United States air or surface commercial carriers under such conditions as may be prescribed by the head of the agency concerned.

2. Other Areas, Vessels, Military Postal Service, Aircraft. Secret information and material may be transmitted from, to or within areas other than those specified in 1. above, by one of the means established for Top Secret information and material, by captains or masters of vessels of United States registry under contract to an agency of the Executive Branch, by United States registered mail through Army, Navy or Air Force Postal Service facilities provided that material does not at any time pass out of United States citizen control and does not pass through a foreign postal system, and by commercial aircraft under charter to the United States and military or other government aircraft.

3. Canadian Government Installations. Secret information and material may be transmitted to and between United States Government and Canadian Government installations in the fifty States, the

District of Columbia and Canada by United States and Canada by United States and Canada registered mail with registered mail receipt.

(d) Transmittal of Confidential. Confidential information and material shall be transmitted within the forty-eight contiguous states and the District of Columbia, or wholly within Alaska, Hawaii, the Commonwealth of Puerto Rico, or a United States possession, by one of the means established for higher classifications, or by certified or first class mail when prescribed by an agency head. Outside these areas, Confidential information and material shall be transmitted only as is authorized for higher classifications.

(e) Transmission within an Agency. Agency regulations governing the preparation and transmission of classified information within an Agency shall ensure a degree of security equivalent to that prescribed above for transmission outside the Agency.

(f) Telecommunications Conversations. Classified information shall not be communicated over telecommunications circuits or systems other than those specifically authorized for transmission of classified information pursuant to subsection (6)(b) above.

(7) Loss or Possible Compromise. Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to an official designated by his Agency or organization. In turn, the originating Agency shall be notified about the loss or possible compromise in order that a damage

assessment may be conducted and appropriate measures taken to negate or minimize the adverse effect of such a compromise. An immediate inquiry shall be initiated by the Agency under whose cognizance the loss or compromise occurred for the purpose of taking corrective measures and appropriate administrative, disciplinary, or legal action.

(8) Destruction. Non-record classified information or material which has served its intended purpose shall be destroyed in accordance with procedures and methods approved by the head of the Agency. The method of destruction selected must preclude recognition or reconstruction of the classified information or material.

Section G. Implementation and Review.

(1) Oversight Office and Committee. In carrying out its functions, the Security Information Oversight Office, established by Section 7(a)(1) of the Order, will place particular emphasis on overseeing compliance with and implementation of the Order and programs established thereunder by each agency in possession of classified information. The Oversight Office shall assist agencies to develop means to (i) avoid overclassification, (ii) ensure prompt declassification in accordance with the provisions of the Order, (iii) facilitate access to declassified information, (iv) avoid unauthorized disclosure of classified information and (v) familiarize agency personnel with the provisions of the Order and this Directive. Members of the Interagency Security Information

Advisory Committee established under Section 7(a)(2) of the Order shall be senior representatives of the agencies identified therein.

(2) Agencies. Members of agency committees established pursuant to Section 7(b)(4) of the Order shall be appointed from among senior agency officials knowledgeable concerning the security classification system established by the Order and significantly responsible for implementation of it within the agency. In accordance with Section 7(b)(10) of the Order, each agency identified in Section 2(d) of the Order shall submit to the Security Information Oversight Office a narrative report concerning the agency's implementation of the Order, this Directive and related matters such as security education and training, significant declassification actions, results of monitoring activities, reduction of classified inventories, and other significant actions. The first of such reports shall cover the period from the effective date of the Order to December 31, 1978, and shall be submitted to the Oversight Office within thirty days thereafter. Subsequent reports shall be submitted on a semiannual basis as above.

Section H. Combat Operations. The provisions of the Order and this Directive with regard to dissemination, transmission, or safeguarding of classified information or material may be so modified in connection with combat or combat-related operations as the Secretary of Defense may by regulations prescribe.

Section I. Atomic Energy Material. "Restricted Data" and material designated as "Formerly Restricted Data" shall be handled, protected, classified, downgraded and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, the Order, this Directive, and the regulations of the Department of Energy issued pursuant to the Act.

Section J. Publication and Effective Date. This Directive shall be published in the Federal Register and become effective March 1, 1978.